Cisco IOS Flexible NetFlow の概要

NetFlow は、ルータを流れるパケットの統計情報が得られる Cisco IOS 技術の 1 つです。NetFlow は、IP ネットワークから実際の IP データを取得するための標準規格です。NetFlow を利用すると、ネットワークとセキュリティの監視、ネットワーク計画、トラフィック分析、および IP アカウンティングを可能にするデータが得られます。

Flexible NetFlow は、実際の要件に合わせてトラフィック分析パラメータをカスタマイズする機能を追加することで、以前の NetFlow よりも改善されています。Flexible NetFlow では、トラフィック分析のための非常に複雑な構成を作成したり、再利用可能な構成コンポーネントを使用してデータをエクスポートすることが容易になります。

このモジュールでは、Flexible NetFlow の概要、および Flexible NetFlow の高度な機能とサービスについて説明します。

機能情報の検索

このモジュールに記載されている機能の一部が、ご使用のソフトウェア リリースでサポートされていない場合があります。最新の機能情報および警告については、ご使用のプラットフォームおよびソフトウェア リリースのリリースノートを参照してください。

プラットフォームのサポート、ならびに Cisco IOS および Catalyst OS ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

マニュアルの内容

Flexible NetFlow について

ここでは、Flexible NetFlow について説明します。

NetFlow の一般的ユーザ

一般的に、NetFlow は次のような、重要なカスタマー アプリケーションのいくつかで使用されます。

- ネットワーク モニタリング。NetFlow のデータを利用すると、広範囲なリアルタイムに近いネットワーク モニタリング機能が可能になります。ネットワーク事業者では、フロー ベースの分析技術を使用して、各ルータおよびスイッチに関連するトラフィック パターン、およびネットワーク全体のトラフィック パターンを視覚化し（集約トラフィックまたはアプリケーション ベースのビューを提供）、積極的な問題検出、効率的なトラブルシューティング、迅速な問題解決を提供しています。
- アプリケーションの監視とプロファイリング。NetFlow のデータを利用すると、ネットワーク マネージャはネットワーク全体における、アプリケーション使用状況を時間ベースで詳細に調べることができます。この情報をプランニング、新しいサービスの理解、ネットワークおよびアプリケーション リソースの割り当てに使用すると（たとえば、Web サーバのサイズ決定、Voice over IP（VoIP）の導入など）、カスタマーの要求にタイミングよく適合できます。
- ユーザの監視とプロファイリング。NetFlow のデータを利用すると、ネットワーク エンジニアはカスタマーおよびユーザによる、ネットワークおよびアプリケーション リソースの使用状況を詳細に理解できます。この情報は、効率的なプランニング、およびアクセス、バックボーン、アプリケーション リソースの割り当てに使用したり、潜在的なセキュリティおよびポリシー違反の検出と解決に使用できます。
- ネットワーク プランニング。NetFlow を使用して、長期間に渡ってデータをキャプチャすると、ネットワークの成長を追跡および予測し、ルーティング デバイス、ポート、および広帯域インターフェイスの数を増加するアップグレードを計画できるようになります。NetFlow サービスのデータを利用すると、ピアリング、バックボーンのアップグレード、ルーティング ポリシーに対するネットワーク プランニングを最適化できます。NetFlow は、ネットワーク運用の総コストを削減しながら、ネットワーク パフォーマンス、機能、および信頼性を高めるために役立ちます。NetFlow では、不要な WAN トラフィックを検出し、帯域幅と QoS（Quality of Service）を検証し、新しいネットワーク アプリケーションの分析を行うことができます。NetFlow からは、ネットワークの運用コストを削減するための有用な情報が得られます。
- セキュリティ分析。NetFlow は、分散型 DoS（dDoS）攻撃、ウイルス、およびワームをリアルタイムに識別および分類します。異常を示すネットワーク動作の変化は、Flexible NetFlow のデータに明確に示されます。このデータは、セキュリティ インシデントの履歴を理解および再現するための有用なフォレンジック ツールにもなります。
- 請求とアカウンティング。NetFlow のデータは、非常に柔軟で詳細なリソース使用量へのアカウンティング用として、きめ細かな計測（たとえば、IP アドレス、パケットおよびバイト数、タイムスタンプ、タイプ オブ サービス（ToS）、アプリケーション ポートなどを含んだ詳細なフロー デー

タ）を提供します。サービス プロバイダーは、時刻、使用帯域幅、アプリケーション使用量、QoS などに基づいた請求に、この情報を使用できます。企業カスタマーは、部門別の経費処理や、リソース使用量に対するコスト割り当てに、この情報を使用できます。

- NetFlow データの保管とデータ マイニング。NetFlow のデータ（または、そこから得られた情報）を保管し、後から取り出して分析することで、積極的なマーケティングおよびカスタマー サービス プログラムをサポートできます（たとえば、内部および外部ユーザが、どのアプリケーションとサービスを使用しているかを調べ、サービスの向上、広告などをそのユーザ向けにターゲティングできます）。また、Flexible NetFlow のデータを利用すると、企業およびサービス プロバイダーに関する「誰が」、「何を」、「どこで」、「どれだけの時間」という情報に、市場調査員がアクセスできます。

以前の NetFlow と Flexible NetFlow でのフロー使用

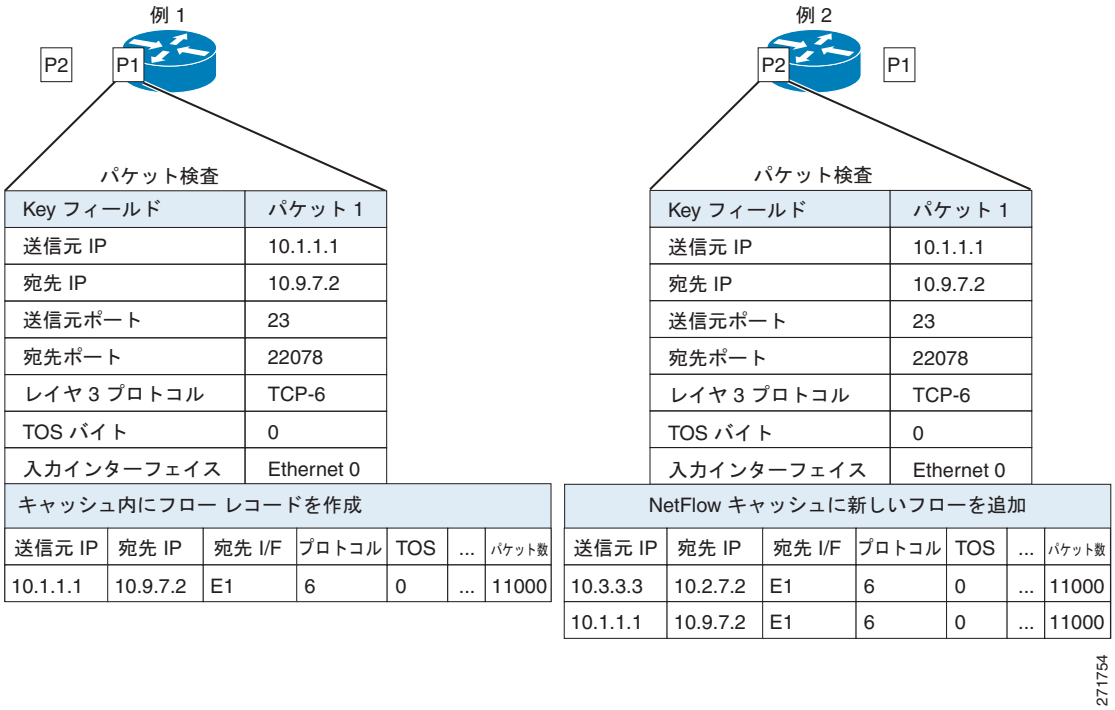
以前の NetFlow と Flexible NetFlow は、どちらも次の概念を使用しています。*フロー*とは、ある送信元とある宛先との間のパケット ストリームと定義されます。

以前の NetFlow と Flexible NetFlow はどちらも、IP 送信元または宛先アドレス、送信元または宛先転送プロトコル ポートなどの IP データグラム内の key フィールドを、ネットワーク トラフィックの監視中にキャッシュ内で新しいフローを作成するタイミング決定の基準として使用します。データグラム内の key フィールドのデータ値が、既存のフローに対して固有の場合、新しいフローが作成されます。

以前の NetFlow および Flexible NetFlow はどちらも、フローからキャプチャされたデータのフィールドを判定する基準として、nonkey フィールドを使用します。フローには、nonkey フィールドの値からキャプチャされたデータが格納されます。

図 1 に、パケットを検査し、キャッシュ内のフロー レコードを作成するプロセスの例を示します。この例では、送信元および宛先 IP アドレス key フィールドの値が異なっているため、キャッシュ内に 2 つの固有のフローが作成されます。

図 1　　パケット検査



以前の NetFlow と Flexible NetFlow

以前の NetFlow は、フローの判定に固定 7 タプルの IP 情報を使用していました。Flexible NetFlow では、フローをユーザ定義できます。Flexible NetFlow の利点としては、次のものがあります。

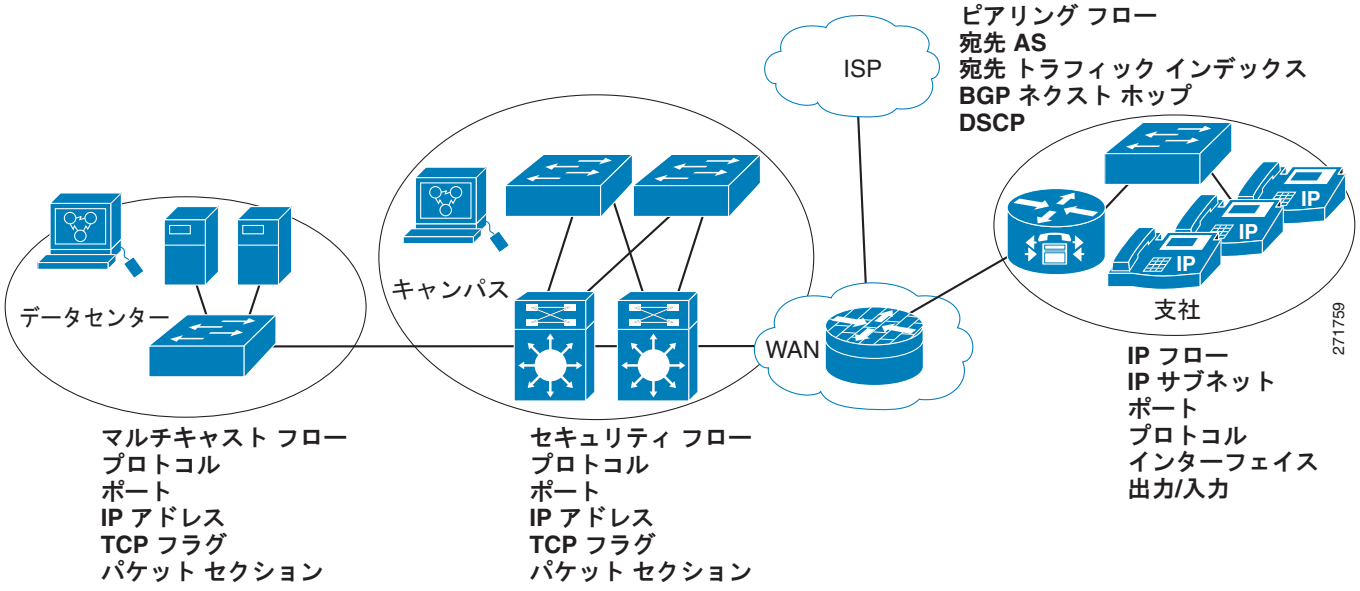
- スケーラビリティ、フロー情報の集約などの、大容量フロー認識。
- セキュリティ監視、および dDoS の検出と識別のための、拡張されたフロー インフラストラクチャ。
- ネットワーク内の特定のサービスまたは動作にフロー情報を適合可能な、パケットの新情報。使用可能なフロー情報は、Flexible NetFlow ユーザがカスタマイズできます。
- シスコの柔軟で拡張可能な NetFlow バージョン 9 エクスポート フォーマットの広範囲な使用。
- IP アカウンティング、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）ポリシー アカウンティング、持続性キャッシュなど、多くのアカウンティング機能に代わるものとして使用可能な、総合的 IP アカウンティング機能。

以前の NetFlow では、ネットワーク内のアクティビティを知ることができたため、ネットワーク設計を最適化し、運用コストを削減できました。Flexible NetFlow では、ネットワーク内で使用されるさまざまなサービス向けにカスタマイズされたフロー情報を使用して、さらに効率よくネットワーク動作を知ることができます。Flexible NetFlow 機能向けのアプリケーション例を、次に示します。

- Flexible NetFlow は、Cisco NetFlow をセキュリティ監視ツールとして拡張します。たとえば、パケット長または MAC アドレスに対して新しいフロー キーを定義すると、ユーザは特定のタイプの攻撃をネットワーク内で検索できます。
- Flexible NetFlow を使用すると、パケット内の CoS で特定の TCP または User Datagram Protocol（UDP）アプリケーションを追跡し、ホスト間でどれだけの量のアプリケーション トラフィックが送信されているかを簡単に知ることができます。
- Multi Protocol Label Switching（MPLS）または IP コア ネットワークに流入し、各ネクスト ホップの宛先が CoS に従うトラフィックのアカウンティング。この機能では、全域におよぶトラフィック マトリクスを作成できます。

図 2 に、ネットワーク内への Flexible NetFlow の導入方法の例を示します。

図 2　　Flexible NetFlow の代表的な導入



Flexible NetFlow のコンポーネント

Flexible NetFlow は、複数の組み合せで使用し、トラフィック分析とデータ エクスポートを実行可能なコンポーネントで構成されます。ユーザ定義のフロー レコード、および Flexible NetFlow のコンポーネント構造によって、ネットワーク デバイスのトラフィック分析およびデータ エクスポートのためのさまざまなコンフィギュレーションを、最小限のコンフィギュレーション コマンドで作成できます。それぞれのフロー モニタは、固有の組み合せのフロー レコード、フロー エクスポータ、およびキャッシュ タイプを持ちます。フロー エクスポータの宛先 IP アドレスなど、パラメータ変更を行うと、そのフロー エクスポータを使用するすべてのフロー モニタで自動的に変更されます。一部のフロー モニタは、さまざまなフロー サンプラと組み合せて使用でき、さまざまなインターフェイスで同じタイプのネットワーク トラフィックを、さまざまなレートでサンプリングできます。ここでは、Flexible NetFlow のコンポーネントについてさらに詳しく説明します。

レコード

Flexible NetFlow では、key および nonkey フィールドの組み合せを *レコード*と呼びます。Flexible NetFlow のレコードは Flexible NetFlow フロー モニタに割り当てられ、フロー データの格納に使用されるキャッシュが定義されます。Flexible NetFlow には事前定義済みのレコードがいくつか含まれ、Flexible NetFlow を簡単に使用開始できるようになっています。Flexible NetFlow の全機能を使用するには、次のセクションで説明するカスタム レコードを作成する必要があります。

NetFlow の事前定義済みレコード

Flexible NetFlow には事前定義済みのレコードがいくつか含まれ、それを使用してネットワーク トラフィックの監視を開始できます。事前定義済みレコードは、Flexible NetFlow を手軽に導入できるよう用意され、ユーザ定義のフロー レコードよりも使いやすくできています。ネットワーク モニタリングのニーズに適した既存の定義済みレコードのリストから、選択できるようになっています。Flexible NetFlow が進化するにつれて、一般的なユーザ定義のフロー レコードが事前定義済みレコードとして利用できるようになり、実装が容易になっています。

事前定義済みレコードは、データがエクスポートされた、既存の NetFlow コレクタ構成との下位互換性を確保するためのものです。事前定義済みレコードは、それぞれ固有の key および nonkey フィールドの組み合せを持ち、ルータで Flexible NetFlow をカスタマイズしなくても、ネットワーク内のさまざまなタイプのトラフィックを監視する、内蔵機能を提供します。

2 つの事前定義済みレコード（NetFlow original と NetFlow IPv4/IPv6 original output）は機能的に同等で、以前の（入力）NetFlow、および以前の NetFlow の 出力 NetFlow アカウンティング機能をそれぞれエミュレートします。その他の Flexible NetFlow 事前定義済みレコードの中には、以前の NetFlow にあった集約キャッシュ スキームに基づいているものがあります。以前の NetFlow にあった集約キャッシュ スキームに基づく Flexible NetFlow 事前定義済みレコードは、集約を実行しません。その代わりに、それぞれのフローが事前定義済みレコードによって個別に追跡されます。

Flexible NetFlow 事前定義済みレコードの詳細については、「Getting Started with Configuring Cisco IOS Flexible NetFlow」モジュールまたは「Configuring Cisco IOS Flexible NetFlow with Predefined Records」モジュールを参照してください。

ユーザ定義レコード

Flexible NetFlow では、key および nonkey フィールドを指定し、実際の要件に合わせてデータ収集をカスタマイズすることで、Flexible NetFlow フロー モニタ キャッシュ用の独自のレコードを定義できます。Flexible NetFlow フロー モニタ キャッシュ用の独自のレコードを定義した場合、そのレコードは*ユーザ定義レコード*と呼ばれます。nonkey フィールドの値がフローに追加され、フロー内のトラフィックに関する追加情報が得られます。nonkey フィールドの値を変更しても、新しいフローは作成されません。多くの場合、nonkey フィールドの値は、フローの最初のパケットだけから取得されます。Flexible NetFlow では、フロー内のバイト数やパケット数などのカウンタ値を、nonkey フィールドとしてキャプチャできます。

ユーザ定義レコードは、QoS および帯域幅監視、アプリケーションとユーザのトラフィック プロファイリング、dDoS 攻撃に対するセキュリティ監視などのアプリケーション用に作成できます。Flexible NetFlow には、以前の NetFlow をエミュレートする事前定義済みレコードも、いくつか含まれています。

Flexible NetFlow のユーザ定義レコードは、サイズをユーザ設定可能なパケットの連続セクションを監視する機能を持ち、それをフロー レコード内で key または nonkey フィールドとして、パケットの他のフィールドおよびアトリビュートと組み合せて使用できます。このセクションには、パケットの任意のレイヤ 3 データを含めることもできます。

パケット セクション フィールドを使用すると、Flexible NetFlow の事前定義済みキーの対象とならないすべてのパケット フィールドを、ユーザが監視できます。事前定義済みキーで収集されないパケット フィールドの分析機能によって、さらに詳細なトラフィック モニタリングが可能になるため、dDoS 攻撃の調査に役立ち、URL モニタリングなど他のセキュリティ アプリケーションの実装が可能になります。

Flexible NetFlow には、サイズをユーザ設定可能な、事前定義済みタイプのパケット セクションが用意されています。次の Flexible NetFlow コマンド（Flexible NetFlow フロー レコード コンフィギュレーション モードで使用）を使用すると、事前定義済みタイプのパケット セクションを設定できます。

- **collect ipv4 section header size** *bytes* : 各パケットの IPv4 ヘッダーの先頭から、*bytes* 引数で指定されたバイト数のキャプチャを開始します。
- **collect ipv4 section payload size** *bytes* : 各パケットの IPv4 ヘッダーの直後のバイトのキャプチャを開始します。キャプチャされるバイト数は *bytes* 引数で指定されます。
- **collect ipv6 section header size** *bytes* : 各パケットの IPv6 ヘッダーの先頭から、*bytes* 引数で指定されたバイト数のキャプチャを開始します。
- **collect ipv6 section payload size** *bytes* : 各パケットの IPv6 ヘッダーの直後のバイトのキャプチャを開始します。キャプチャされるバイト数は *bytes* 引数で指定されます。

bytes 値は、フロー レコード内のフィールドのバイト サイズです。対応するパケットのフラグメントが、要求されたセクション サイズよりも小さかった場合、Flexible NetFlow はフロー レコードのセクション フィールドの残りを 0 で埋めます。パケット タイプが要求されたセクション タイプと一致しなかった場合、Flexible NetFlow はフロー レコード内のセクション フィールド全体を 0 で埋めます。

Flexible NetFlow では、ヘッダーおよびパケット セクション タイプとして、新しいバージョン 9 エクスポート フォーマット フィールド タイプが追加されています。Flexible NetFlow は、対応するバージョン 9 エクスポート テンプレート フィールドに設定されたセクション サイズについて、NetFlow コレクタと通信します。ペイロード セクションは対応する長さフィールドを持つことがあり、収集されたセクションの実際のサイズの収集に使用されます。

フロー モニタ

フロー モニタは、ネットワーク トラフィック モニタリングを実行するためインターフェイスに適用される、Flexible NetFlow コンポーネントです。フロー モニタは、ユーザ定義または事前定義済みレコード、オプションのフロー エクスポータ、およびフロー モニタが最初のインターフェイスに適用されたときに自動作成されるキャッシュで構成されます。フロー データはネットワーク トラフィックから収集され、モニタリング プロセス中にフロー レコード内の key および nonkey フィールドに基づいて、フロー モニタ キャッシュに追加されます。

Flexible NetFlow は、同じトラフィックのさまざまなタイプの分析実行に使用できます。図 3 ではパケット 1 が、標準トラフィック分析用に設計されたレコードを使用して、入力インターフェイスで分析され、セキュリティ分析用に設計されたレコードを使用して、出力インターフェイスで分析されます。

図 3　　2 つのフロー モニタを使用した同一トラフィック分析の例

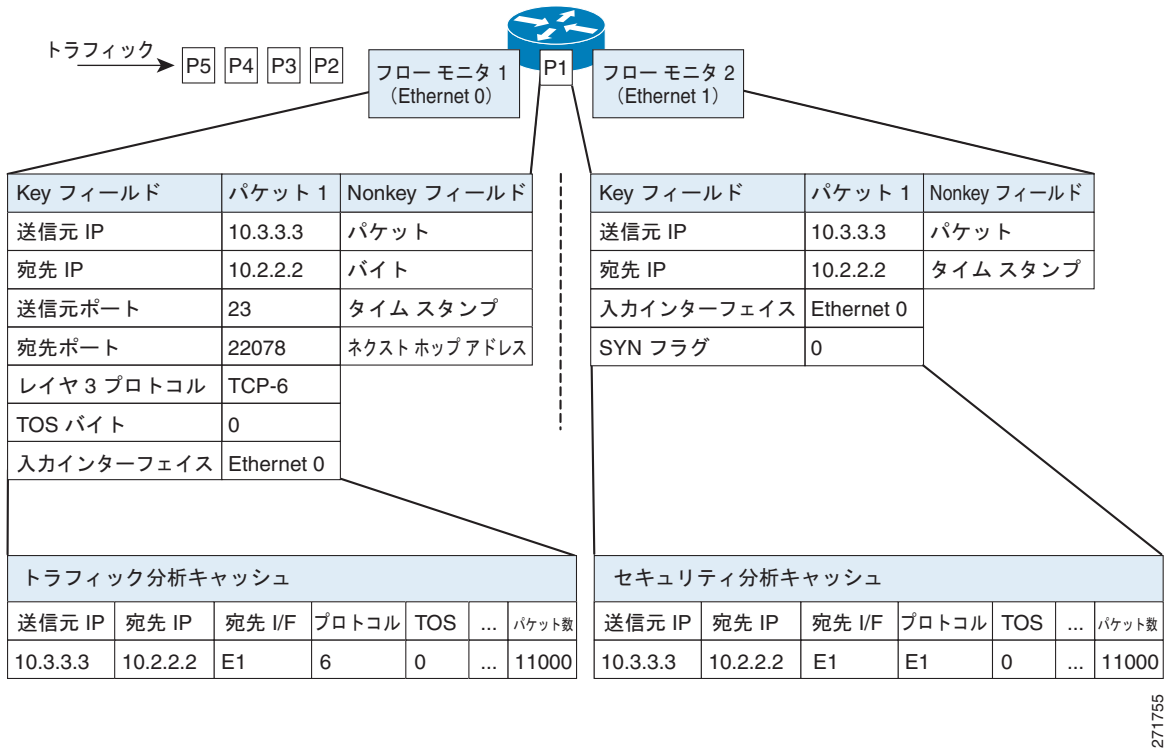
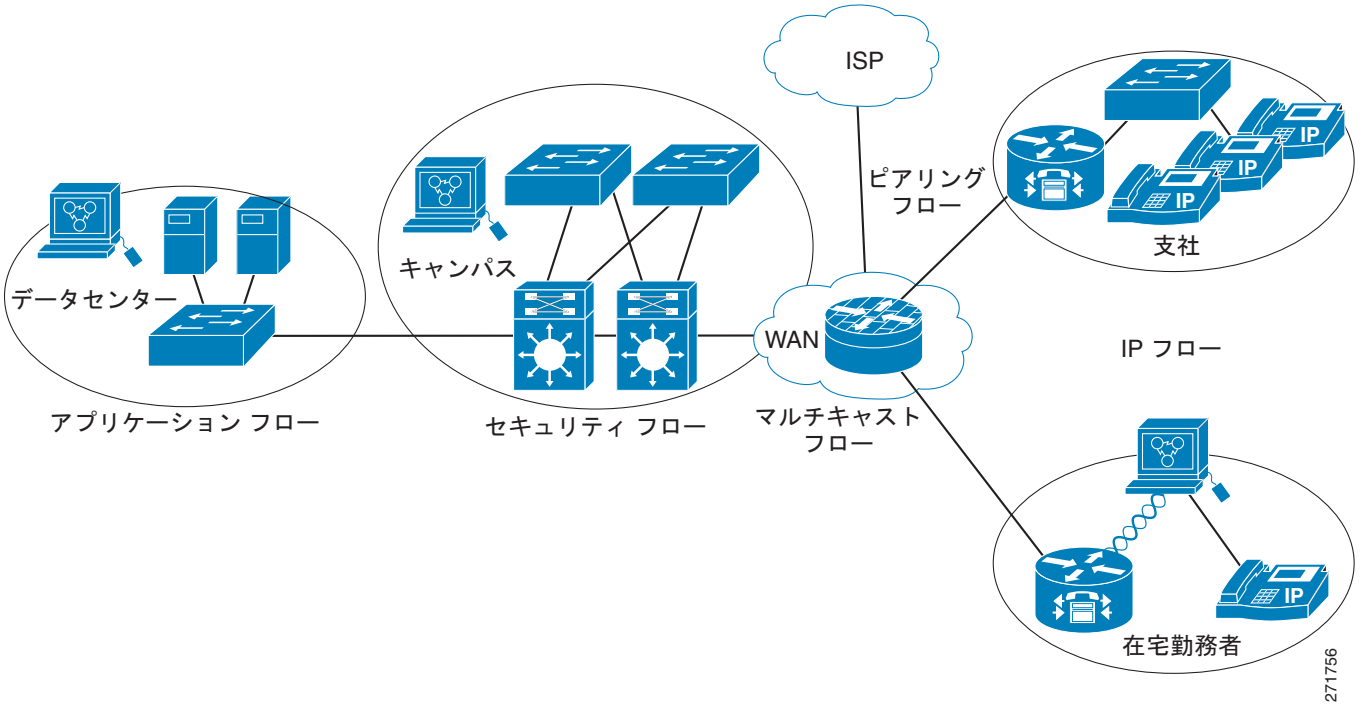


図 4 は、カスタム レコードを持つさまざまなタイプのフロー モニタを適用する方法の、少し複雑な例を示しています。

図 4　　カスタム レコードを持つ複数タイプのフロー モニタを使用する複雑な例



3 つのタイプのフロー モニタ キャッシュがあります。フロー モニタで使用されるキャッシュのタイプは、フロー モニタの作成後に変更できます。3 タイプのフロー モニタ キャッシュについては、次の各項に説明があります。

- 「Normal」（P.8）
- 「Immediate」（P.8）
- 「Permanent」（P.9）

Normal

デフォルトのキャッシュ タイプは「normal」です。このモードでは、キャッシュ内のエントリが timeout active と timeout inactive の設定に従って期限切れになります。キャッシュ エントリは、期限切れになるとキャッシュから削除され、設定されている何らかのエクスポータによってエクスポートされます。

Immediate

タイプが「immediate」のキャッシュでは、レコードがクリアされるとすぐに、そのレコードが期限切れになります。その結果、各フローにはパケットが 1 つだけ含まれます。キャッシュ内容を表示するコマンドでは、パケットの履歴が表示されます。

予想されるフローが非常に少なく、パケットが検出されてからレポートがエクスポートされるまでの遅延を最小限にする場合は、このモードが適しています。

注意 このモードではエクスポート データの量が多くなるため、低速リンクが過負荷になったり、エクスポート先のシステムに負担がかかることがあります。サンプリングを設定し、処理されるパケット数を減らすようにしてください。

（注） キャッシュのタイムアウト設定は、このモードに影響を与えません。

Permanent

タイプが「permanent」のキャッシュでは、フローが期限切れになりません。permanent キャッシュは、検出が予想されるフローの数が少なく、ルータに長期間の統計情報を保存する必要がある場合に便利です。たとえば、フロー レコード内の key フィールドが 8 ビット IP ToS フィールドだけで、256 フローだけを監視する場合があります。ネットワーク トラフィックの IP ToS フィールドの使用状況を長期間に渡って監視するには、permanent キャッシュを使用します。permanent キャッシュは、課金アプリケーション、および追跡対象が固定セットのフローに対する、全域におよぶトラフィック マトリクスに役立ちます。アップデート メッセージは、「timeout update」設定に従って設定されたすべてのフロー エクスポータに、定期的に送信されます。

（注） permanent モードでキャッシュがいっぱいになった場合は、新しいフローが監視されなくなります。そうなった場合は、キャッシュの統計情報に「Flows not added」というメッセージが示されます。

（注） permanent キャッシュでは、デルタ カウンタではなくアップデート カウンタが使用されます。そのため、フローがエクスポートされると、カウンタにはフローのライフタイム全体の総検出数が示され、最後のエクスポート送信後に検出された追加パケットは示されません。

フロー エクスポータ

フロー エクスポータは、フロー モニタ キャッシュ内のデータを、NetFlow コレクタが稼動するサーバなどのリモート システムにエクスポートし、分析および保存されるようにします。フロー エクスポータは、設定内に独立したエンティティとして作成されます。フロー エクスポータはフロー モニタに割り当てられ、フロー モニタのデータ エクスポート機能を提供します。複数のフロー エクスポータを作成し、それを 1 つ以上のフロー モニタに割り当てると、複数のエクスポート先を提供できます。フロー エクスポータを 1 つ作成し、それを複数のフロー モニタに適用することもできます。

NetFlow データ エクスポート フォーマット バージョン 9

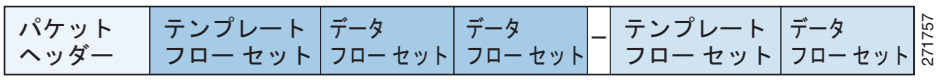
NetFlow の基本出力はフロー レコードです。NetFlow の完成度が高まるにつれて、いくつかのフォーマットのフロー レコードが開発されました。NetFlow エクスポート フォーマットの最新の進化は、バージョン 9 と呼ばれます。NetFlow バージョン 9 エクスポート フォーマットの特長的機能は、テンプレート ベースであることです。テンプレートは、レコード フォーマットの設計を拡張可能なものにします。NetFlow サービスが将来拡張されても、基本フロー レコード フォーマットを変更し続ける必要がありません。テンプレートを使用すると、次のような利点が得られます。

- NetFlow 用のコレクタまたは表示サービスを提供するアプリケーションを作成しているサードパーティ ビジネス パートナーは、NetFlow の新機能が追加されるたびに、アプリケーションを再コンパイルする必要がありません。代わりに、既知のテンプレート フォーマットが記述された、外部データ ファイルを使用できます。
- 現在の実装を無駄にすることなく、NetFlow に新機能を簡単に追加できます。

- NetFlow は、新規または開発中のプロトコルに対して「将来性」を持っています。バージョン 9 フォーマットでは、そうしたプロトコルのサポートに対応できるからです。

バージョン 9 エクスポート フォーマットは、パケット ヘッダーと、それに続く 1 つ以上のテンプレート フローまたはデータ フロー セットで構成されます。テンプレート フロー セットは、将来のデータ フロー セットに含まれるフィールドの説明を提供します。こうしたデータ フロー セットは、同一エクスポート パケット内、または後続のエクスポート パケット内で、後から発生することがあります。テンプレート フロー セットは、図 5 に示すように、単一エクスポート パケット内に混在できます。

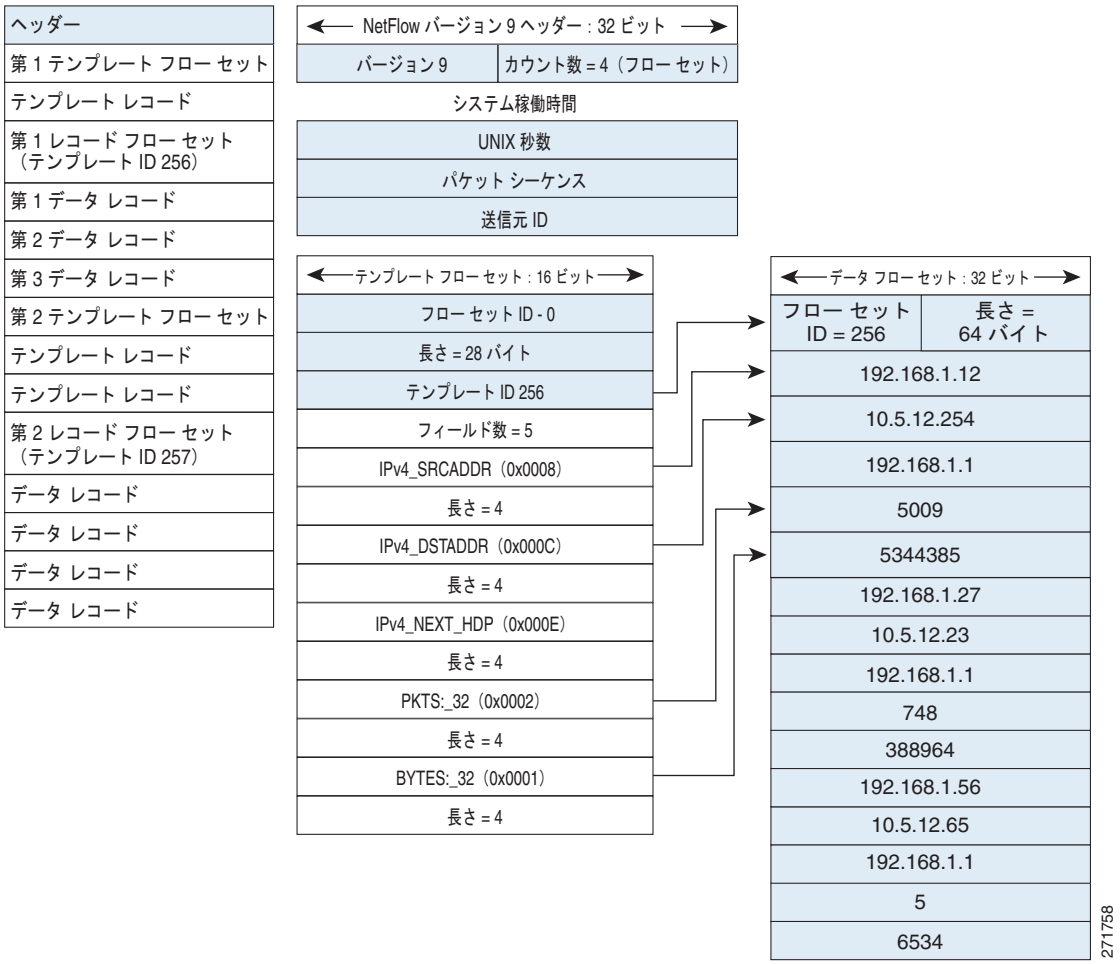
図 5　　バージョン 9 エクスポート パケット



NetFlow バージョン 9 は定期的にテンプレート データをエクスポートし、NetFlow コレクタはどのデータ セットが送信されるかを把握し、テンプレートのデータ フロー セットもエクスポートします。Flexible NetFlow にとっての大きな利点は、ユーザがフロー レコードを設定すると、それが効率的にバージョン 9 テンプレートに変換されて、コレクタに転送されることです。図 6 は、ヘッダー、テンプレート フロー、データ フロー セットなどの、NetFlow バージョン 9 エクスポート フォーマットの詳細な例を示しています。

（注） NetFlow バージョン 5 エクスポート フォーマットは、Flexible NetFlow データの限定的な情報を提供する、固定エクスポート フォーマットです。そのため、Flexible NetFlow ではバージョン 9 エクスポート フォーマットが使用されます。

図 6　NetFlow バージョン 9 エクスポート フォーマットの詳細な例



バージョン 9 エクスポート フォーマットの詳細については、『*Cisco IOS NetFlow Version 9 Flow-Record Format*』というタイトルのホワイト ペーパーを参照してください。このドキュメントは、http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper09186a00800a3db9.shtml から入手できます。

フロー サンプラ

フロー サンプラは、分析対象のパケット数を制限することで、Flexible NetFlow によってネットワーク デバイスにかかるトラフィック監視の負荷を軽減するために使用されます。サンプリングのレートは、2 ～ 32,768 の範囲のパケット数分の 1 に設定できます。たとえば、サンプリングレートを 2 分の 1 にすると、50% のパケットがネットワーク デバイスでの分析で処理されます。

フロー サンプラは、フロー モニタと組み合せてインターフェイスに適用され、Flexible NetFlow のフロー サンプリングが実装されます。パケットは、指定されたレートでサンプラで分析され、フロー モニタに関連付けられたフロー レコードと比較されます。分析されたパケットが、フロー レコードで指定された基準に適合している場合、そのパケットはフロー モニタ キャッシュに追加されます。

Flexible NetFlow によるセキュリティ監視

Flexible NetFlow は、IP ヘッダー全体、さらにはパケット セクションを追跡し、この情報をフローに反映する機能を持つため、ネットワーク攻撃検出ツールとして使用できます。セキュリティ監視システムでは、Flexible NetFlow のデータを分析し、ネットワーク内で問題が検出されると、仮想バケットまたは仮想キャッシュを作成してトラフィック固有の情報に設定して、攻撃パターンまたはワーム伝播の詳細を識別できます。特定の情報でキャッシュを動的に作成する機能を、入力フィルタリングと組み合せると（特定の宛先への全フローのフィルタリングなど）、Flexible NetFlow を強力なセキュリティ監視ツールにすることができます。

よくあるタイプの攻撃としては、TCP フラグを使用して宛先サーバに TCP 要求を大量に送り付けるというものがあります（SYN フラッド攻撃など）。攻撃側デバイスは、ある宛先に TCP SYN のストリームを送信しますが、TCP 3 ウェイ ハンドシェイクの中で、サーバの SYN-ACK への応答としての ACK は送信しません。セキュリティ検出サーバが必要とする、宛先アドレスまたはサブネット、TCP フラグ、パケット カウントという、3 つの重要フィールドを得るためには、フロー情報が必要です。セキュリティ検出サーバは一般的な Flexible NetFlow 情報を監視しますが、Flexible NetFlow がルータの設定内に動的に新しいフローを作成することで、このデータによってこの攻撃の詳細な状態が判明することがあります。新しいフロー モニタには、どのトラフィックを Flexible NetFlow キャッシュで認識できるようにするかを制限するフィルタリング、および TCP ベースの攻撃を診断するための情報の追跡が含まれます。この場合、ユーザはサーバの宛先アドレスまたはサブネットへのすべてのフロー情報をフィルタリングし、セキュリティ検出サーバが評価する必要のある情報量を制限することがあります。セキュリティ検出サーバで、この攻撃が判明したと判断された場合、そのサーバは別のフロー モニタをプログラムし、パケットのペイロード情報またはセクションを収集およびエクスポートして、パケットに含まれる痕跡を詳細に調べます。これは、セキュリティ インシデントの検出に Flexible NetFlow を使用する、多数の例の 1 つにすぎません。

以前の NetFlow と Flexible NetFlow の機能比較

表 1 に、以前の NetFlow と Flexible NetFlow の機能ごとの比較を示します。

表 1　以前の NetFlow と Flexible NetFlow の機能ごとの比較

機能	以前の NetFlow	Flexible NetFlow	説明
NetFlow Data Capture	サポートあり	サポートあり	データ キャプチャは、Flexible NetFlow の事前定義済みおよびユーザ定義レコード内で使用できます。Flexible NetFlow には、以前の NetFlow のトラフィック分析機能をエミュレートする事前定義済みキーが、いくつか含まれています。
NetFlow Data Export	サポートあり	サポートあり	フロー エクスポータは、Flexible NetFlow フロー モニタ キャッシュからリモート システムに、データをエクスポートします。
NetFlow for IPv6	サポートあり	サポートあり	IPv6 サポートは、Cisco IOS リリース 12.4(20)T で以前の NetFlow から削除されました。 Flexible NetFlow—IPv6 Unicast Flows 機能は、Flexible NetFlow の IPv6 サポートとして Cisco IOS リリース 12.4(20)T で実装されました。

表 1　以前の NetFlow と Flexible NetFlow の機能ごとの比較 （続き）

機能	以前の NetFlow	Flexible NetFlow	説明
MPLS-Aware NetFlow	サポートあり	サポートなし	—
MPLS Egress NetFlow	サポートあり	サポートあり	Flexible NetFlow—MPLS Egress NetFlow 機能は、Flexible NetFlow の MPLS NetFlow 出力サポートとして Cisco IOS リリース 12.4(22)T で実装されました。
NetFlow BGP Next Hop Support	サポートあり	サポートあり	Flexible NetFlow レコードの事前定義済みキーおよびユーザ定義キーに使用できます。
Random Packet Sampled NetFlow	サポートあり	サポートあり	Flexible NetFlow サンプリングで使用できます。
NetFlow v9 Export Format	サポートあり	サポートあり	Flexible NetFlow エクスポータで使用できます。
NetFlow Subinterface Support	サポートあり	サポートあり	Flexible NetFlow モニタをサブインターフェイスに割り当てられます。
NetFlow Multiple Export Destinations	サポートあり	サポートあり	Flexible NetFlow エクスポータで使用できます。
NetFlow ToS-Based Router Aggregation	サポートあり	サポートあり	Flexible NetFlow レコードの事前定義済みレコードおよびユーザ定義レコード内で使用できます。
NetFlow Minimum Prefix Mask for Router-Based Aggregation	サポートあり	サポートあり	事前定義済みレコードおよびユーザ定義レコード内で使用できます。
NetFlow Input Filters	サポートあり	サポートなし	—
NetFlow MIB	サポートあり	サポートなし	—
NetFlow MIB and Top Talkers	サポートあり	サポートなし	—
NetFlow Multicast Support	サポートあり	サポートあり	Cisco IOS Release 12.4(9)T から 12.4(20)T の Flexible NetFlow は、マルチキャスト フローの統計情報を収集します。ただし、バイトおよびパケットのレプリケーション カウントなど、一部の追加フィールドはサポートされません。 Flexible NetFlow—IPv4 Multicast Statistics Support 機能は、バイトおよびパケットのマルチキャスト レプリケーション カウントのキャプチャ サポートとして、Cisco IOS Release 12.4(22)T で実装されました。
NetFlow Layer 2 and Security Monitoring Exports	サポートあり	一部サポートあり	Flexible NetFlow—Layer 2 Fields 機能は、MAC アドレスおよび仮想 LAN（VLAN）ID キャプチャ サポートとして、Cisco IOS Release 12.4(22)T で実装されました。

表 1　以前の NetFlow と Flexible NetFlow の機能ごとの比較 （続き）

機能	以前の NetFlow	Flexible NetFlow	説明
Egress NetFlow Accounting	サポートあり	サポートあり	Flexible NetFlow モニタを使用すると、インターフェイスおよびサブネット上の出力トラフィックを監視できます。
NetFlow Reliable Export with SCTP	サポートあり	サポートなし	—
NetFlow Dynamic Top Talkers CLI	サポートあり	サポートあり	Flexible NetFlow—Top N Talkers Support 機能は Cisco IOS Release 12.4(22)T で実装され、同じ機能を提供します。

次の作業

以前の NetFlow のトラフィック分析およびデータ エクスポートをエミュレートする、Flexible NetFlow の基本設定を実装する方法については、「Getting Started with Configuring Cisco IOS Flexible NetFlow」モジュールを参照してください。その他の Flexible NetFlow 設定の実装方法については、「関連資料」（P.15）を参照してください。

参考資料

ここでは、Flexible NetFlow に関する参考資料について説明します。

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
Flexible NetFlow の機能ロードマップ	「Cisco IOS Flexible NetFlow Features Roadmap」
Flexible NetFlow による以前の NetFlow のエミュレーション	「Getting Started with Configuring Cisco IOS Flexible NetFlow」
Flexible NetFlow データをエクスポートするためのフロー エクスポータの設定	「Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters」
実際のネットワーク用の Flexible NetFlow のカスタマイズ	「Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors」
Flexible NetFlow のトラフィック監視によるオーバーヘッド軽減のためのフロー サンプリング設定	「Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic」
事前定義済みレコードを使用した Flexible NetFlow の設定	「Configuring Cisco IOS Flexible NetFlow with Predefined Records」
Flexible NetFlow Top N Talkers を使用したネットワーク トラフィックの分析	「Using Cisco IOS Flexible NetFlow Top N Talkers to Analyze Network Traffic」
Flexible NetFlow 用の IPv4 マルチキャスト統計情報サポートの設定	「Configuring IPv4 Multicast Statistics Support for Cisco IOS Flexible NetFlow」
Flexible NetFlow のコンフィギュレーション コマンド	『*Cisco IOS Flexible NetFlow Command Reference*』

RFC

RFC	タイトル
RFC 3954	『*Cisco Systems NetFlow Services Export Version 9*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html